互联网根服务器系统
The Root Server System

保罗 霍夫曼 （Paul Hoffman）, ICANN 首席技术专家

北京网络安全大会（Beijing Cyber Security Conference）
2020年8月12日

引言

- 报告内容将重点围绕“互联网根服务器系统”展开
- 报告内容将假设听众对互联网域名系统有所了解
- 报告内容提纲：关于根服务器系统的六个问题
  - What?
  - Who?
  - Why?
  - How?
  - Where?
  - When?

What: 根区文件包含什么？

- 根区文件中包含全部的域名顶级域（TLDs）
  - 国家/地区顶级域，例如 .cn, .中国, .aq, ...
  - 通用顶级域，例如 .com, .microsoft, .नेट, .nyc, ...
  - 遗留顶级域（.int, ...），基础设施（.arpa, ...）以及用于测试的顶级域
- 根区文件中每个顶级域均包含与之相对应的域名服务器信息，这些信息有助于引导完成层次化的递归解析
- 根区文件中包含资源记录的数字签名记录（DNSSEC协议）；接收方可通过对数字签名内容进行校验，进而判断资源记录的真实性
- 根区文件内容每天均会进行若干次的同步或更新，根区文件的数据源均来自于IANA

What: 名称术语

- 根区文件（Root zone） – 互联网域名系统的顶层数据
- 根服务器运行管理机构（Root server operator，RSO）– 负责管理运营互联网根服务器的组织机构
- 根服务器标识符（Root server identifier） – 与根服务器运行管理机构相对应的域名信息，例如 m.root-server.net
- 根服务器系统（Root server system，RSS） – 部署实现并对外提供根域名服务的服务器节点集合

若需获取更多细节，请参阅 RSSAC026v2, *RSSAC Lexicon*

Who: 根服务器运行管理机构

- 目前12家根服务器运行管理机构，共对应着13个根服务器标识符 （有一家机构同时管理两个根服务器标识符）
- 对于每个根服务器运行管理机构，在选择服务器类型、DNS软件、以及选取根服务器节点的部署位置等方面，均保持着高度独立
- 所有的根服务器运行管理机构都一致同意，只接受由IANA所提供的数据作为根区文件内容
- 从某种程度上说，根服务器运行管理机构是谁并不重要，因为它们所提供的数据内容完全一致。在这一点上，它们极其可靠

Who: 根域名服务所面向的用户群体

- 普通互联网用户并不是根域名服务的直接受众群体
- 根域名服务的用户群体是，互联网运营商以及组织机构所维护的数以百万计的递归解析服务器
- 普通互联网终端用户依赖于递归解析服务器，从根服务器系统中获取及时、准确的解析结果
- 仅有非常少量的互联网用户拥有自己专用的递归解析服务器，这些用户也是根域名服务的受众，但这类用户在群体中占比极小

Why: 运行管理根服务器的缘由

- 12家根服务器运行管理机构，选择积极提供根域名服务的缘由各不相同
- 对于大部分的运行管理机构而言，一个重要的原因是希望互联网更有弹性，更加稳定
- 有些根服务器管理机构是大学，它们收集根服务器的数据进行学术研究；还有些根服务器管理机构是网络服务提供商，它们有着许多类似的服务，等等
- 所有的根服务器运行管理机构都承诺，应当为数以百万计的递归解析服务器提供可靠的域名解析服务，提供一致、正确的应答响应内容

How: 13 个根服务器标识符，1000+ 个根服务器节点

- 互联网域名系统有13个根服务器标识符 （a.root-servers.net, b.root-servers.net, ...），每个根服务器均存在与之对应的IPv4与IPv6主机地址
- 每个根服务器运行管理机构都会采用任播技术（Anycast），使用完全相同的主机地址，在世界各地部署多个根服务器节点
- 任播组中的每个服务器均被称为：根服务器节点（*instance*）
- 根服务器系统中目前拥有超过1000个服务器节点，节点规模仍在不断增加
- 由于根服务器运行管理机构在运营决策上完全独立，因此它们所维护的根服务器节点数量各不相同

How: 如何保障根区文件的安全？

- DNSSEC技术已经被证明，能够为互联网域名系统的区域文件提供行之有效的真实性认证，其中也包含根区文件
- 2010年，DNS根区文件支持DNSSEC签名；目前，绝大多数的顶级域也已支持了DNSSEC签名
- 2018年，用于根区文件签名的秘钥首次更新；几年之后，签名秘钥很可能会再次更新
- 然而，目前递归解析服务器一侧对DNSSEC数字签名的验证比例很低，因此大约仅有三分之一的互联网用户能够从DNSSEC技术中受益

Where: 根服务器节点的位置

- 这些根服务器节点遍布全球各地，包括大城市、偏远的小城市、甚至是岛屿
- 请访问 https://root-servers.org/ ，查看交互式地图，了解所有根服务器节点的地理位置
- 根服务器系统中的1000+ 个服务器节点，基本上能够满足对所有递归解析服务器的域名解析需求，而且不至于对终端用户产生较大的网络延迟
- 众多的根服务器节点，使得域名系统能够更好地应对拒绝服务攻击，因为攻击者产生的流量往往会被分散到不同根服务器节点

When: 在过去的35年时间里

- 在互联网域名系统被发明之前，域名解析服务器便已经存在
- 当域名系统处于起步阶段时，根服务器的数量非常少，全球各地的递归解析服务器只能向少量几个服务器节点发送查询请求
- 直到1997年，现有的13个根服务器标识符开始运行
- 在2002年，为了突破13个根服务器数量的限制，任播技术开始广泛应用，根服务器节点的规模开始增加

若需获取关于根服务器系统演进过程的更多信息，请参阅 RSSAC023v2, *History of the Root Server System*,

When: 当前，以及可预期的未来

- 根服务器系统的运行状况良好，以至于大部分互联网用户未曾察觉到它的存在
- 根服务器节点的规模仍将持续增长
- 即便考虑到COVID-19的影响，DNSSEC签约仪式所创造的数字签名规模也要优于往年
- 我们正在积极制定关于未来如何治理根服务器系统的方案

ICANN 合作与交流

Thank You and Questions

Visit us at **icann.org**
Email: email


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


slideshare/icannpresentations


soundcloud/icann